암호응용서비스

이 병 천

2011. 11. 22

중부대학교 정보보호학과

목차

1. 전자우편 보안

- **전자우편이란**
  - 현재 인터넷 사용자들이 가장 많이 사용하고 있는 인터넷 서비스중의 하나
  - 송신자가 수신자에게 일방향으로 메시지 전달
  - 보안상 매우 취약한 구조를 가지고 있음
    - 프라이버시 문제 : 엽서와 같은 구조
    - 인증 문제 : 남이 내 이름을 빌어 메일을 보낼 수 있음
- **전자우편의 보안요구사항**
  - 기밀성
  - 인증성 (부인방지) : 신분인증, 메시지인증
  - 무결성

보안 기법

- **암호화 : 기밀성 제공**
  - 대칭키 암호화 : 메시지 본문을 암호화
  - 공개키 암호화 : 키를 암호화
- **전자서명 : 인증성 제공**
- **해쉬함수 : 무결성 제공**
- **메시지 압축 : 통신량 감소, 기밀성 향상**
- **사용자 인증 : 상대방의 신분 인증 (신뢰 및 분쟁시 문제 해결)**
  - PKI 이용 : S/MIME 방식
  - 다른 방법 이용 : PGP 방식

전자우편 어플리케이션

- **POP3 소프트웨어:**
  - Outlook, Eudora 등
- **웹메일:**
  - 포털사이트: 네이버메일, 한메일 등
  - 업무용 웹메일

- 기존의 응용계층 소프트웨어에 보안기능을 적용하는 좋은 사례임

- 사용자 인증 방법에 따라
  - PKI 이용 : S/MIME 방식
  - 전통적인 신뢰기법 이용 : PGP 방식

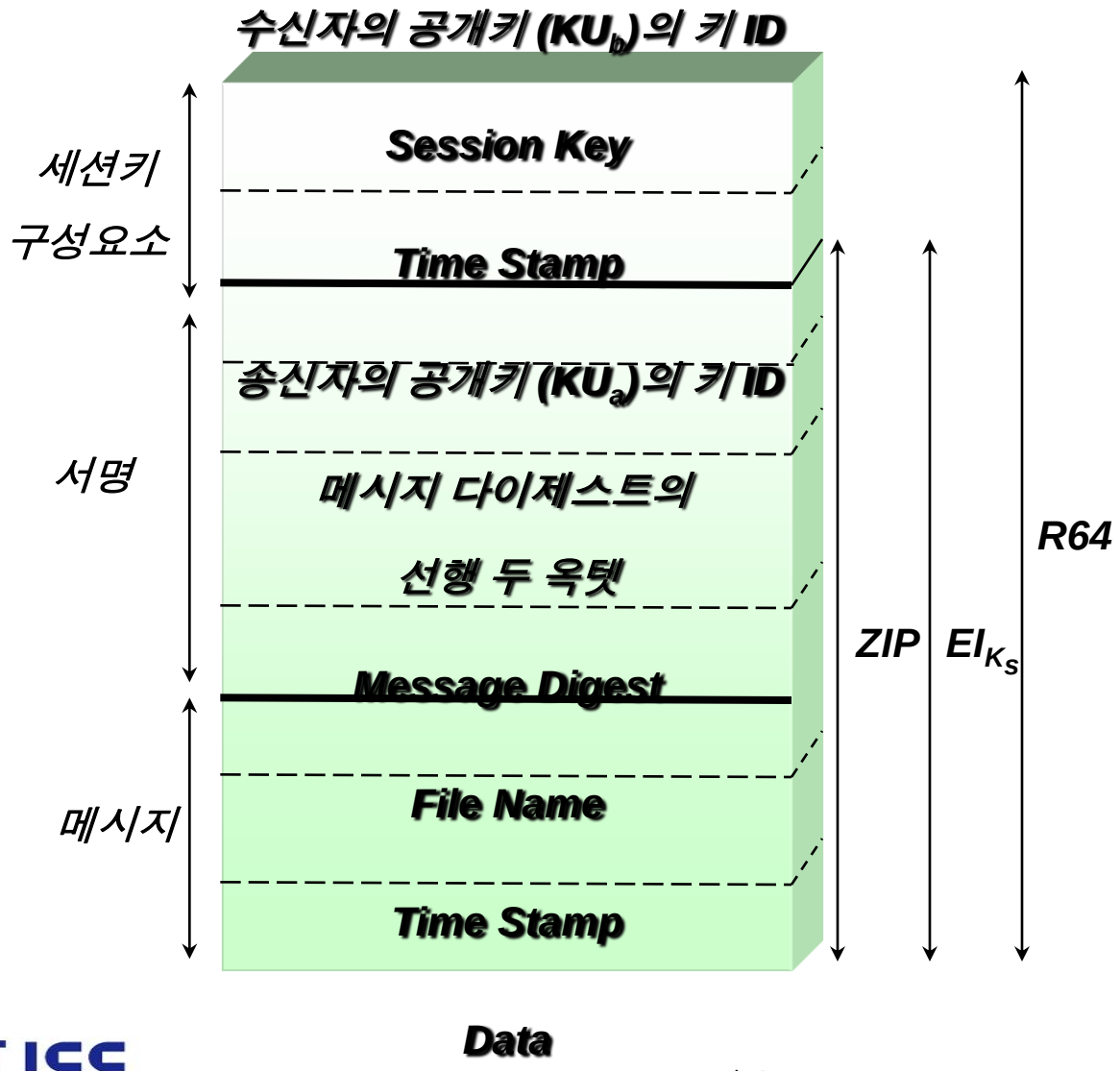
1.1 PGP

- **PGP (Pretty Good Privacy)**
  - 1991년 미국의 Phil Zimmermann에 의해서 개발된 대표적인 전자우편 보안 도구.
  - 구현이 용이하고 일반적으로 사용된 알고리즘의 안전성이 높기 때문에 일반 대중에게 널리 사용.
  - 정부나 특정 단체에서 만든 것이 아니라 개인이 만들어 무료로 배포.
  - 암호화 알고리즘을 이용하여 기밀성, 인증, 무결성, 부인방지 등의 기능을 지원.
  - http://www.pgpi.com

PGP 기능과 사용 암호 알고리즘

기 능	사용 암호 알고리즘
메시지 기밀성	IDEA,CAST,Triple-DES
전자서명 (무결성, 사용자 인증, 송신자 부인 봉쇄)	RSA,DSS/Diffie-Hellman, SHA-1,MD5,RIPEMD-160
압축	ZIP
전자우편 호환성	Radix-64 conversion

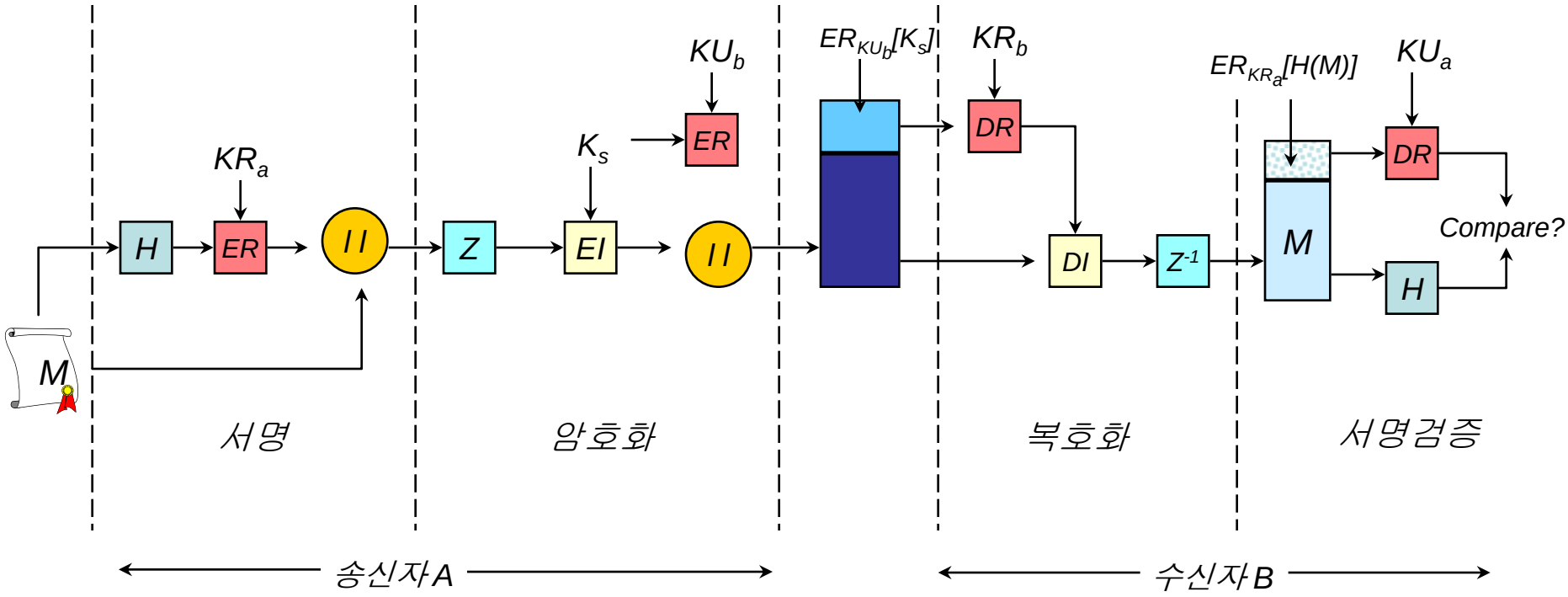
PGP의 메시지의 구조



KUb=사용자 b의 공개키
KUa=사용자 a의 공개키
Ks=세션키
ER=암호화기능
EI=IDEA 복호화 기능
ZIP=PKZIP 압축 기능
R64=Radix-64 변환 기능

PGP의 기능 및 동작

❖ 기밀성 및 인증성 제공



1.2 S/MIME

- **인터넷 전자 메일의 구성**
  - 헤더: 메시지 전송과 관련된 주요 정보
  - 보디: 메시지 내용
- **MIME (Multipurpose Internet Mail Extension)**
  - 보디 부분을 어떻게 구성할 것인가에 대한 정의를 나타낸다.
  - 텍스트 이외의 음성, 영상, 문서, 첨부화일 등을 메일 메시지 형태로 구성하는 방법에 대한 정의
  - MIME 객체
- **S/MIME (Secure MIME)**
  - 응용계층에서 보안을 제공하는 가장 대표적인 시스템
  - MIME 객체에 암호화와 전자서명 기능을 추가한 프로토콜.
  - 전자우편에 국한하여 보안을 제공하지는 않는다.

S/MIME이 제공하는 보안 서비스

보안서비스	보안 메커니즘	암호 알고리즘
메시지 기밀성	암호화	Triple-DES
메시지 무결성	해쉬함수	SHA-1
사용자 인증	공개키 인증	x.509 v3인증서
부인방지	전자 서명	DSA

S/MIME 인증서

❖ S/MIME 인증서

- X.509 인증서에 포함된 공개키를 이용해 보안 메커니즘을 이용

❖ 공개키 인증서 발행 절차

- 사용자는 웹 브라우저를 이용해 인증서 발행 기관에 접속, 이때 자신의 비밀키와 공개키를 만든다.
- 자신의 공개키, 전자우편 주소와 같은 사용자 정보를 작성 및 전송
- 인증기관에서는 X.509 형태의 S/MIME 인증서를 발행.

❖ S/MIME의 동작

- 사용자는 수신자에게 보낼 메시지를 작성 (MIME형태로).
- 전자서명, 암호화, 전자서명/암호화 3개 중 택한다.
- 그러면 S/MIME 어플리케이션은 MIME형태의 메시지를 S/MIME 메시지로 변환한 후 전송
- 수신자는 메일을 복호화, 전자서명 확인 등을 통하여 메일을 확인한다.

전자우편 보안 시스템의 비교

❖

전자우편 보안 시스템	비고
PEM (Privacy Enhanced Mail)	IETF Internet 표준안 중앙 집중화 된 키 인증, 구현이 어렵다 높은 보안성(군사용, 은행 시스템) 많이 사용되지 않음
PGP (Pretty Good Privacy)	Phil Zimmerman 이 개발 분산화 된 키 인증 구현이 용이 일반 용도의 보안성 많이 사용
S/MIME	RSA Data Security,Inc개발 전자우편 메시지 표준(MIME)기반 다양한 상용 툴 킷 x.509인증지원
PGP/MIME	전자우편 메시지 표준(MIME)기반 PGP암호 기법+전자우편 시스템 x.509인증서 지원 안됨

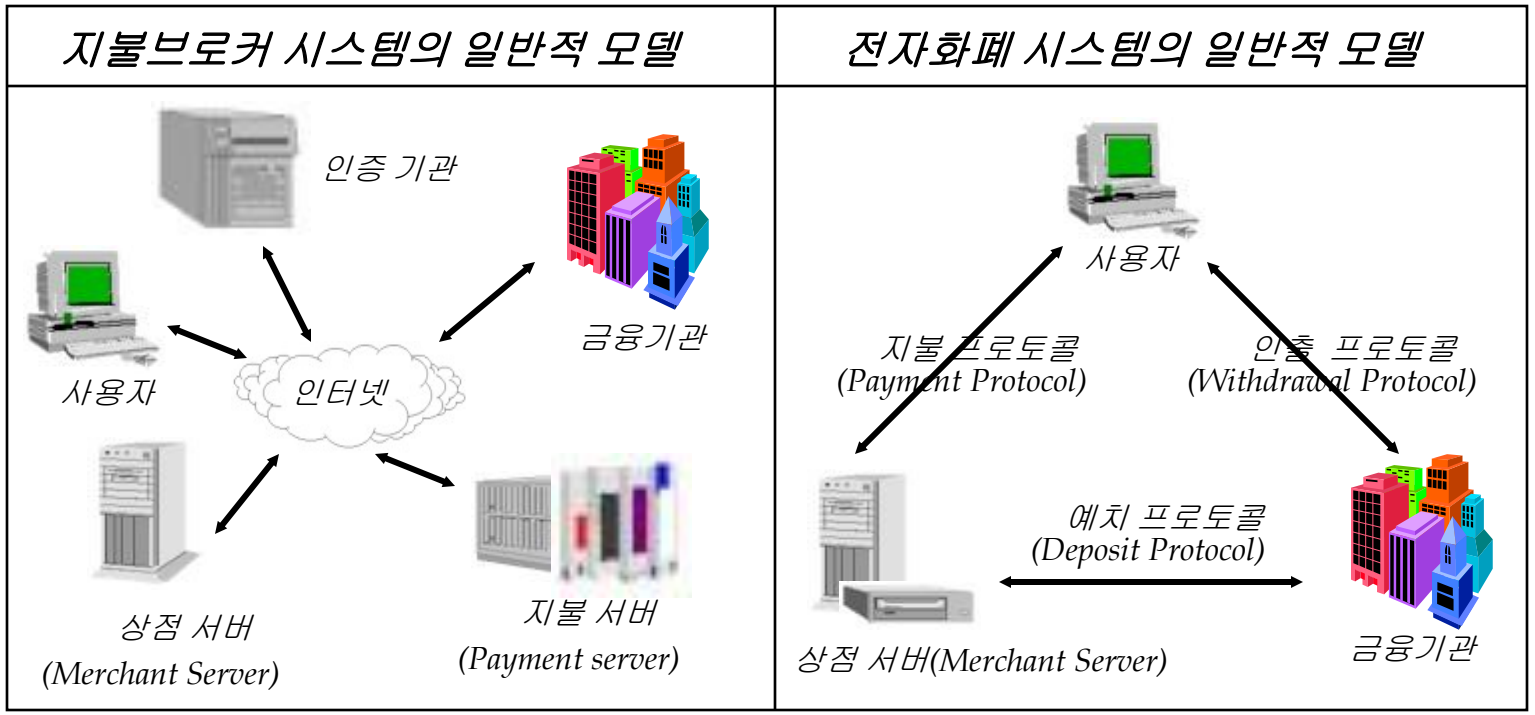
2. 전자지불 시스템

❖ 전자지불 시스템의 분류

- **전자 화폐(*Electronic Cash*) 시스템** : 지불 브로커 없이 독립적인 신용구조를 가짐, 현금과 유사한 개념의 전자적 지불수단
  - 네트워크형 : Ecash, NetCash, Millicent 등
  - IC 카드형 : Mondex
- **지불브로커(*Payment Broker*) 시스템** : 독립적인 신용구조 없이 신용카드나 은행계좌를 이용한 전자적 지불수단
  - 신용카드시스템 : SET, FV 등
  - 전자수표시스템 : NetCheque, Echeck 등

전자지불 시스템

❖ 두 가지 방식의 비교



전자지불 시스템

❖ 두 가지 방식의 비교

지불브로커 시스템	전자화폐 시스템
• 특징 - 독립적 신용 구조를 갖지 않음. - 신용카드, 은행을 이용, 네트워크 상에서 지불하도록 연결하는 구조 - 현실적 전자지불 시스템	• 특징 - 사용자 프라이버시 보호 - 실제 화폐를 대치할 수 있음. - 기밀정보의 노출 위험성 제거 - 오프라인 방식으로 사용 가능
• 단점 - 사용자의 프라이버시 침해 (거래의 추적 가능성) - 기밀정보 (예:신용카드번호) 의 노출 위험성	• 단점 - 몇 가지 이론적 문제들이 잔재 - 전자화폐 시스템을 지원할 수 있는 하드웨어 기술의 부족

2.1 전자화폐

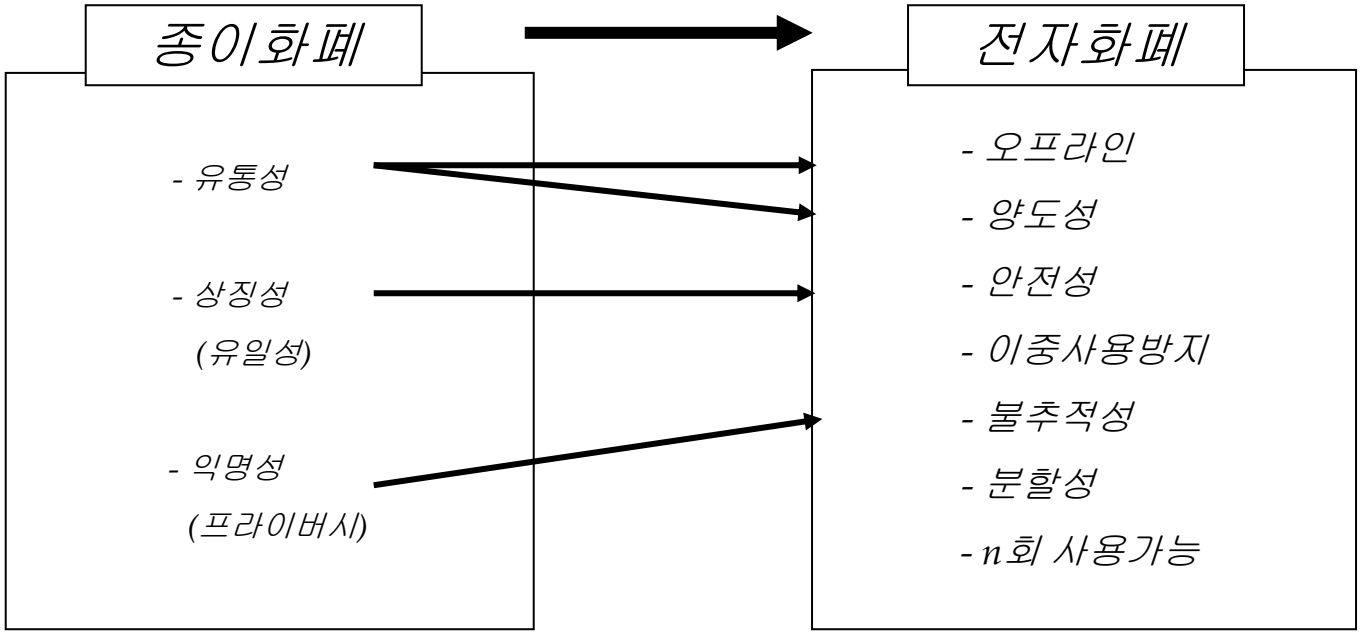
❖ IC카드형

- IC카드에 화폐가치 저장
- 온라인 거래, 오프라인 거래 모두 사용 가능
- 소액결제에 적합, 초기 투자비용이 과다
- 현재의 선불카드를 가치 재충전을 가능하게 하는 동시에 범용성을 가지도록 한 것
- IC 카드형 전자화폐 기술 개발 및 이용이 활발한 유럽에 활성화
- 사례: Mondex, Visa Cash, PC Pay

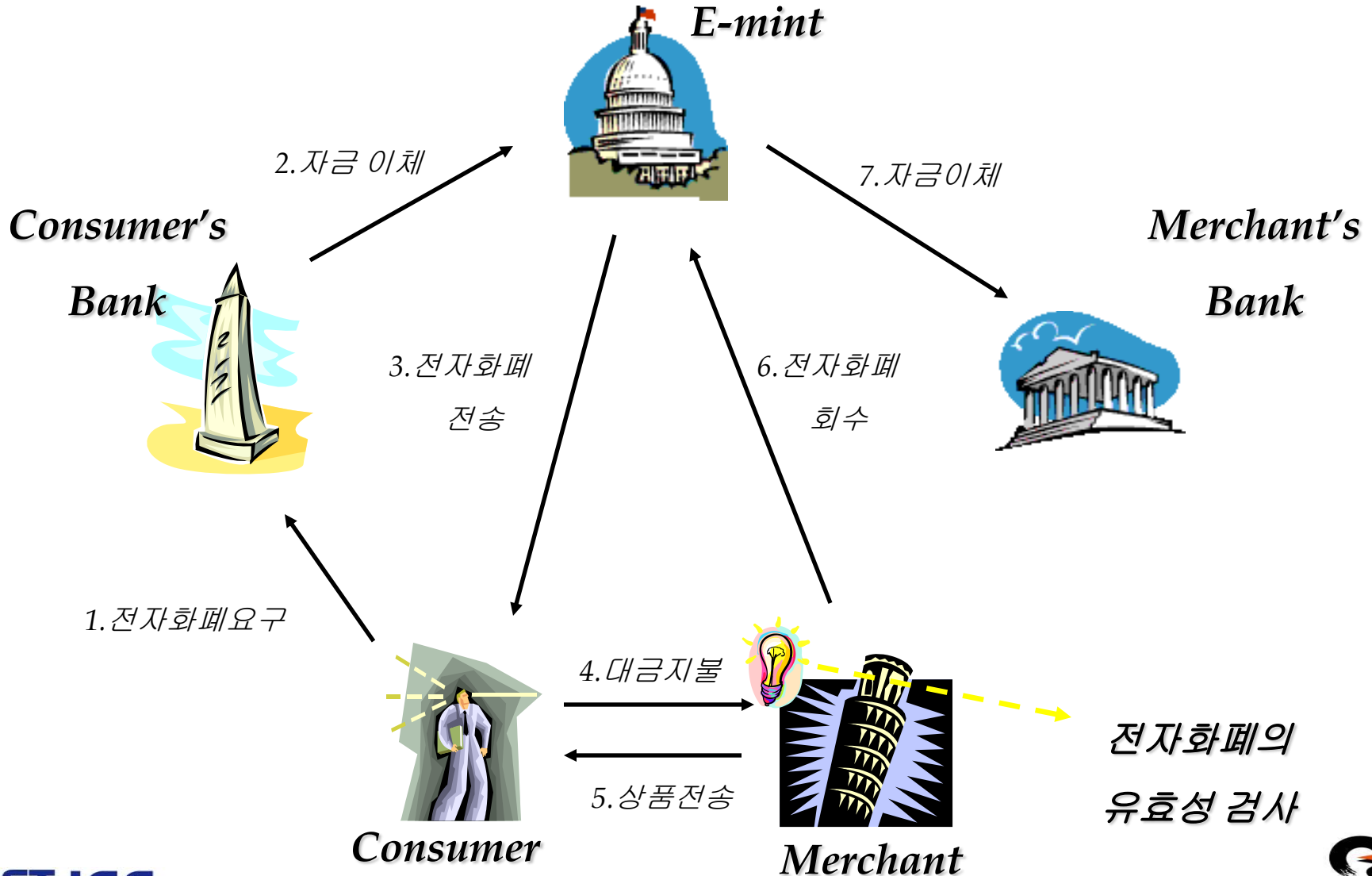
❖ 네트워크형

- 소프트웨어(전자지갑) 다운로드
- 디지털 형태 화폐가치를 네트워크 주고받음
- 사례: e-Cash, NetCash, PayMe
- 온라인 거래에 적합, 초기투자 비용이 저렴
- 컴퓨터의 높은 보급률, 넓은 국토, 통신망의 발달한 미국에 활성화

전자화폐의 보안요구사항



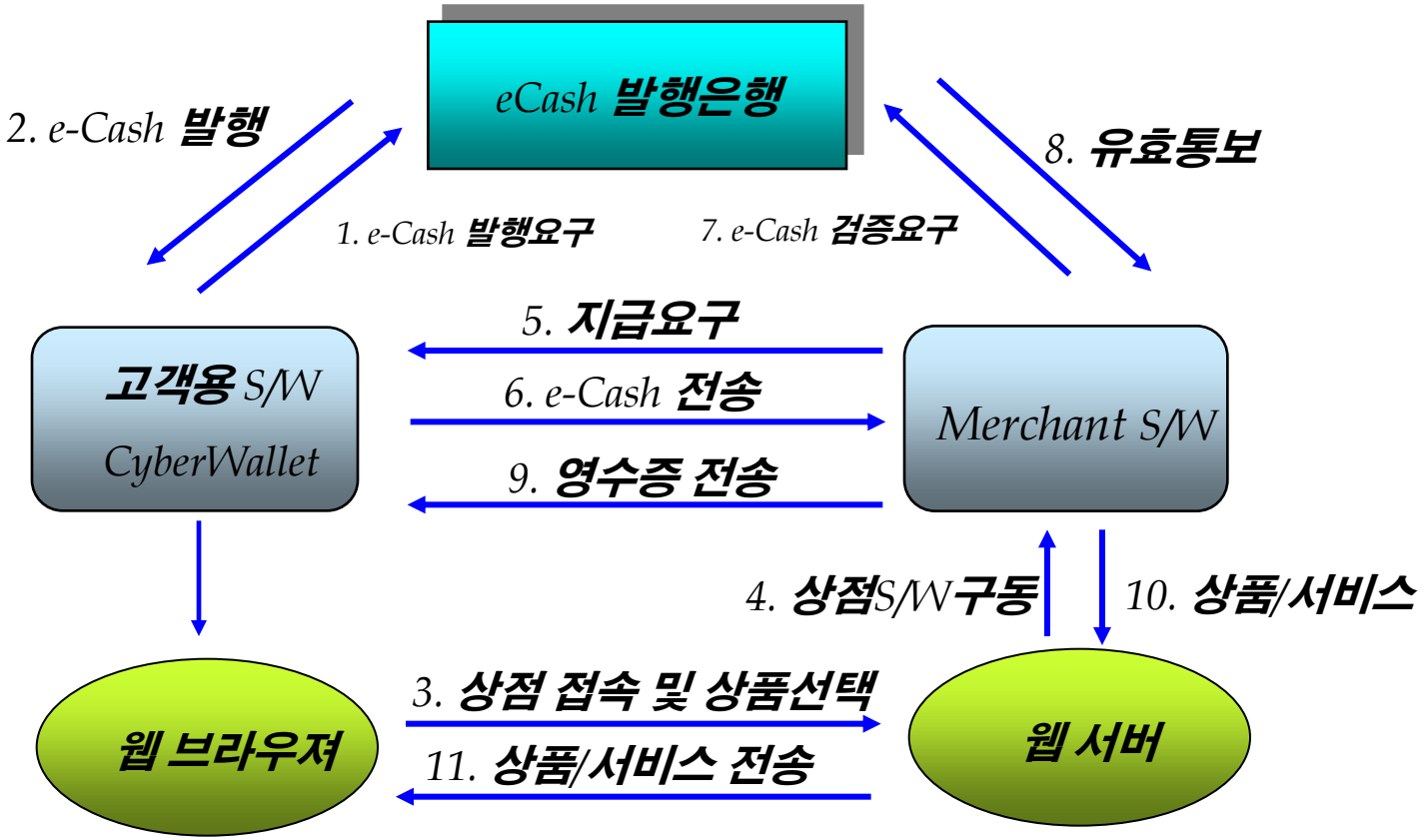
전자화폐의 일반적인 흐름



Ecash

- **DigiCash**사에서 개발 **(**현재 미국 **e-Cash Technology**사에 흡수**)**
- **D. Chaum**의 은닉서명 기술을 이용하여 온라인상에서의 완전한 익명성을 제공
- **RSA** 공개키 암호 방식 이용
- 사용자 전자지갑인 **Cyberwallet**과 **Merchant** 소프트웨어 필요
- 은행은 **e-Cash**의 이중사용 방지를 위하여 기 사용된 **e-Cash** 일련번호를 **DB**로 관리하여야 함

Ecash 흐름도


eCash 발행은행
2. e-Cash 발행
1. e-Cash 발행요구
7. e-Cash 검증요구
8. 유효통보
고객용 S/W
CyberWallet
5. 지급요구
6. e-Cash 전송
9. 영수증 전송
Merchant S/W
4. 상점S/W구동
10. 상품/서비스
웹 브라우져
3. 상점 접속 및 상품선택
11. 상품/서비스 전송
웹 서버

Mondex

- 특징
  - IC 카드형 전자화폐, Off-line 시스템
  - 현금지불의 장점과 카드 지불의 편리함을 결합
  - 개인과의 자금 이체가 자유로움, 개인의 프라이버시 보호
  - 멀토스(MULTOS :Multi-Application Operating System) 를 COS(Chip Operating System) 로 채용
  - 5 개국의 화폐를 동시 저장 및 거래내역 기록 가능
  - 은행을 거치지 않고 카드간 및 개인간 화폐 교환 가능

Mondex

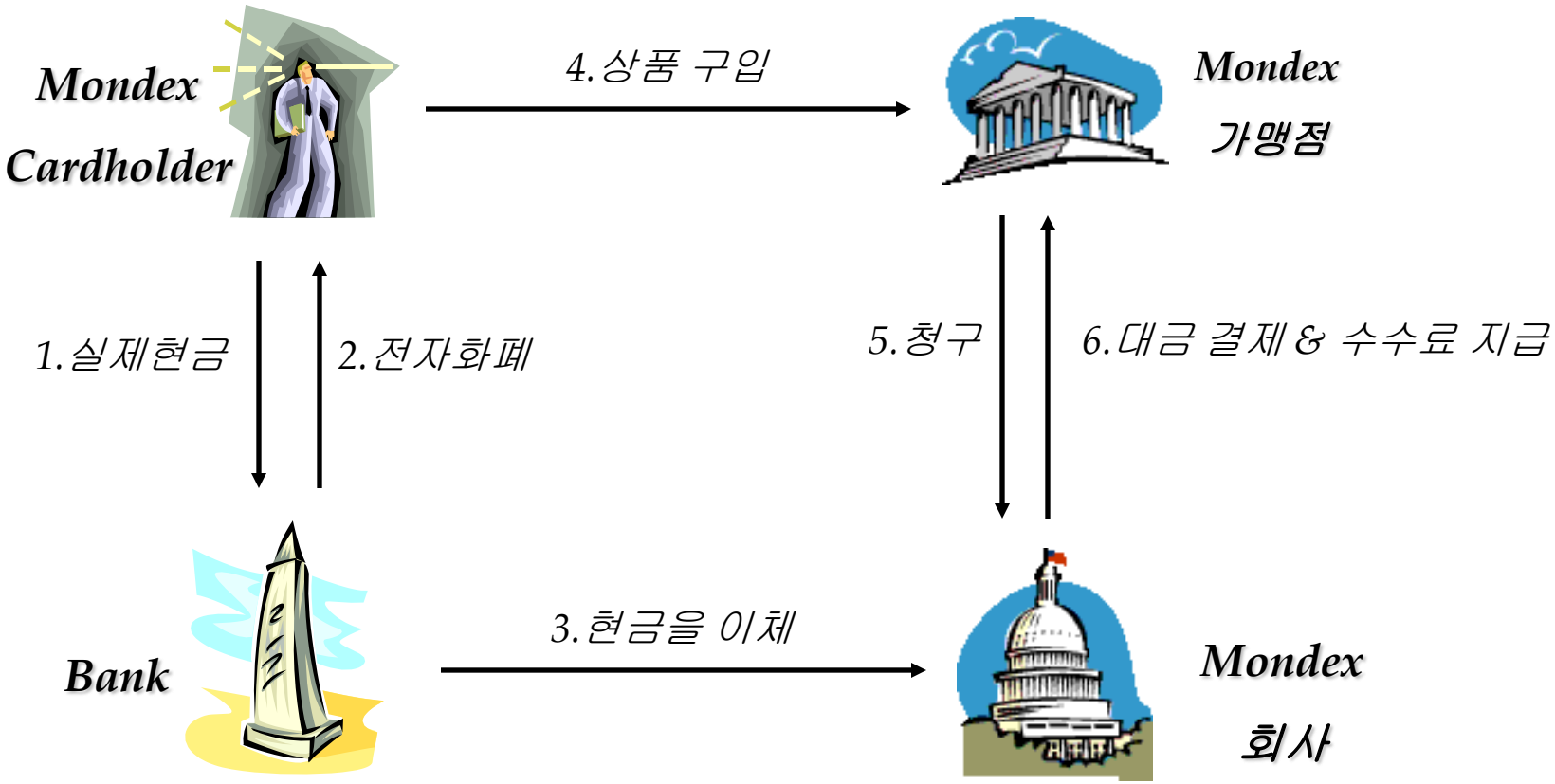
❖ Mondex 구성장비

- Mondex Wallet
  - 소형 IC카드 단말기
  - 카드의 내용 표시나 개인간의 전자화폐이체 기능
  - Mondex 전자화폐를 저장하기도 함
  - 은행이 고객에게 대여

- Mondex Balance Reader
  - 카드에 저장된 잔액을 나타냄

- Mondex Telephone
  - 전화기와 판독 장치를 통합
- Mondex Card
  - 스마트 카드
  - 비밀번호에 의한 보안 기능

Mondex


Mondex
Cardholder
4.상품 구입
Mondex
가맹점
1.실제현금
2.전자화폐
5.청구
6.대금 결제 & 수수료 지급
Bank
3.현금을 이체
Mondex
회사

Visa Cash

- 비자에서 개발한 선불 카드 개념
- **Visa Cash**가 통용되는 **11**개국에서 사용가능
- 인터넷과 같은 개방 네트워크에서 소액지불 수단
  - 형태
    - Disposable Visa Cash
      - ✓ 지하철패스나 버스 카드의 개념
      - ✓ 재사용 불가능
    - Reloadable Visa Cash
      - ✓ 재사용 가능(충전)

PC Pay

- **Innovonics사에서 개발**
- 스마트 카드와 카드 리더기로 구성
- 응용분야
  - 인터넷 뱅킹 서비스
  - 의료 정보 서비스
  - 티켓 구매와 여행 정보 서비스
  - 물품 구매 및 지불 서비스
- 특징
  - Pin-pad(스마트 카드) 유지 : 소프트웨어의 불법접근 제한
  - 카드 리더기에서 PC로 가는 데이터를 암호화 전송
  - DES 이용

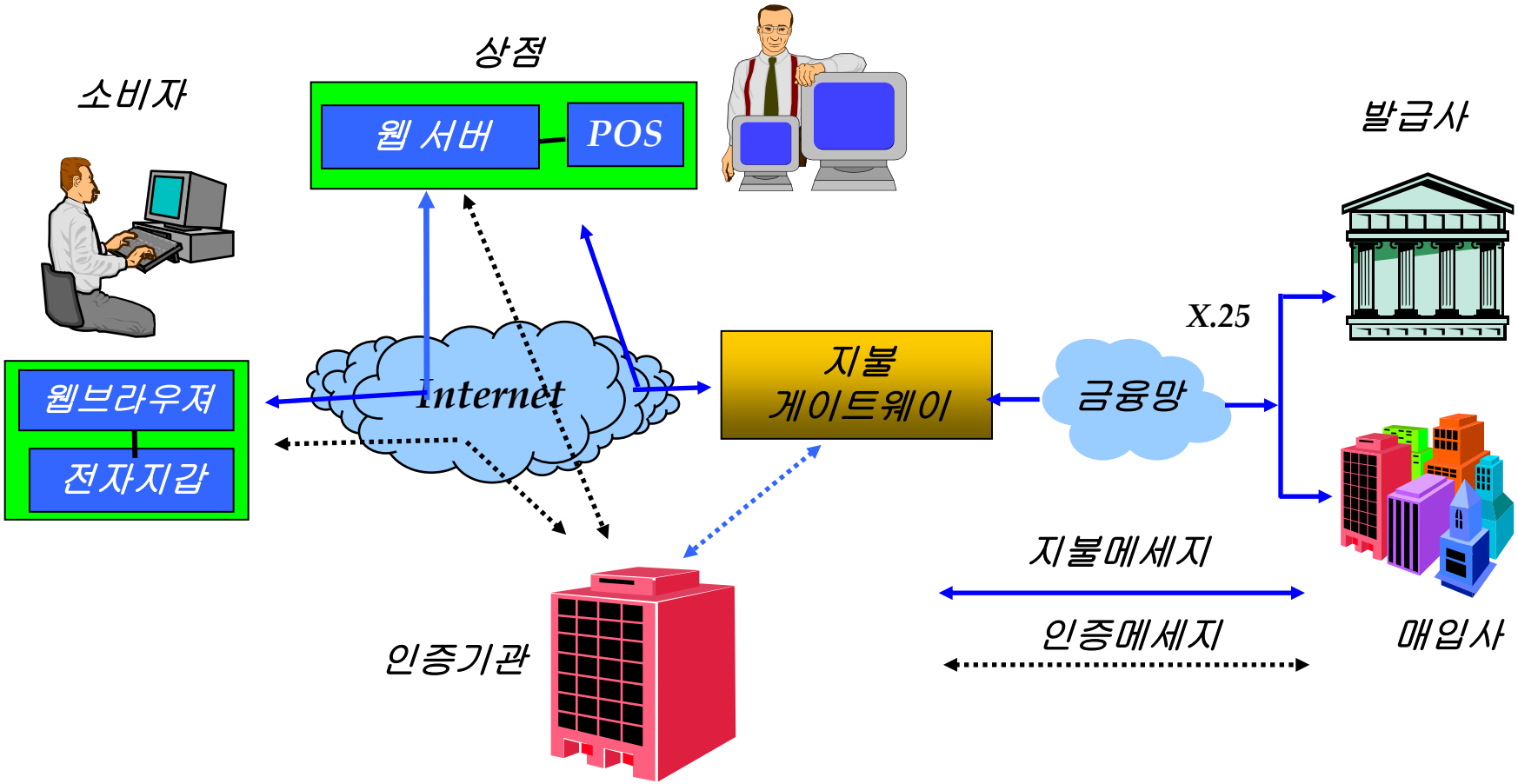
2.2 신용카드 지불시스템

- **SET(Secure Electronic Transaction)**
  - Visa, MasterCard사에 의해 개발된 신용카드 기반의 전자 지불 프로토콜
  - 공개키 기반구조를 바탕으로 사용자 인증을 수행
    - 카드 소유자의 인증
    - 상점의 인증
    - 매입 은행의 인증
  - 지불명령 메시지에 대한 암호화 : 신용카드 정보와 지불정보의 노출 방지
  - 거래 정보의 무결성

SET의 구성요소

- 고객(**Card Holder**) : 카드 소지자
- 상점(**Merchant**) : 인터넷상에서 상품이나 정보서비스 제공자
- 지불 중계기관(**Payment Gateway**) : 판매자가 요청한 고객의 지불정보(카드번호)로 금융기관에 승인 및 결재를 요청하는 자
- 발급사(**Issuer**) : 고객카드를 발급하고 고객계좌가 개설된 금융기관
- 매입사(**Acquirer**) : 상점을 가맹점으로 승인하고 상점계좌가 개설된 금융기관

SET 구성도


소비자
상점
웹 서버
POS
발급사
웹브라우저
전자지갑
Internet
지불
게이트웨이
X.25
금융망
지불메세지
인증메세지
인증기관
매입사

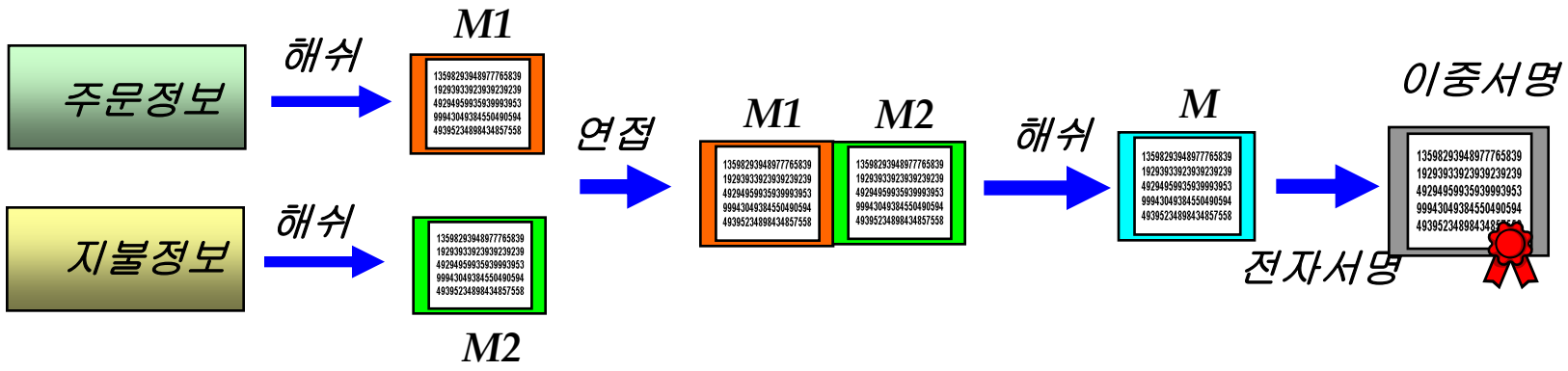
SET에서 사용되는 암호기술

- **비밀키 암호기술(대칭형 암호기술)**
  - 전자문서를 암호화하는데 사용
- **공개키 암호기술(비대칭형 암호기술)**
  - 암호화에 사용된 비밀키는 공개키 암호방식으로 암호화하여 키분배 문제 해결
- **전자봉투 (Digital Envelope)**
  - 송신자의 전자문서를 암호화에 사용한 비밀키를 수신자만이 볼 수 있도록 수신자의 공개키(키 교환용 공개키)로 암호화 한 것 (키 분배문제 해결)
- **전자서명(Digital Signature)**
  - 서명자 인증, 전자문서 위.변조 방지, 부인방지 목적으로 활용
- **해쉬함수**
  - 임의의 길이 전자문서(평문)를 일정한 길이의 코드 값(160 비트의 축약문(Message Digest)으로 만듬

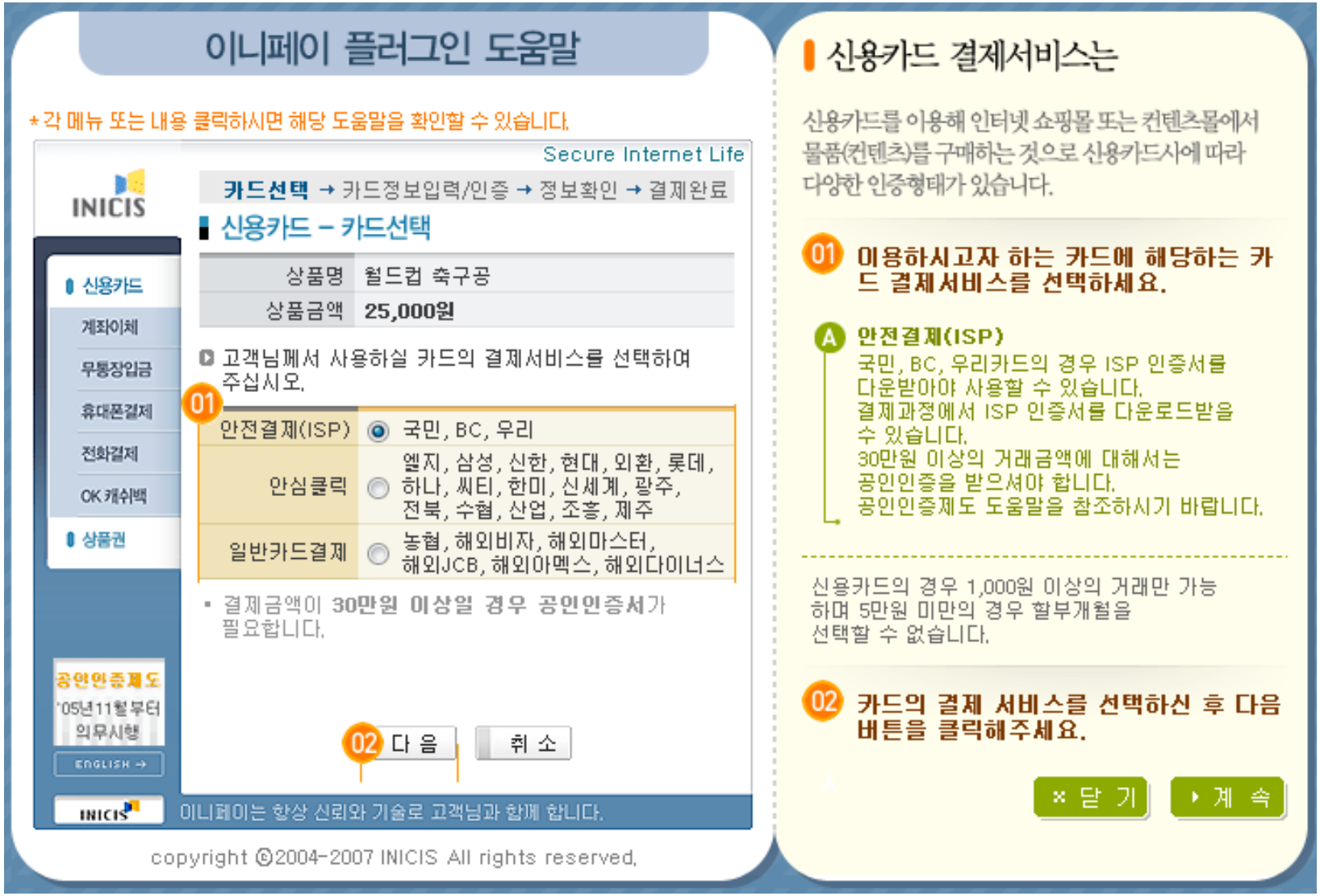
SET에서 사용되는 암호기술

❖ 이중서명

- 사용자의 지불정보를 상점에게 숨기고 주문 정보는 은행에게 숨김
- 지불정보(카드번호)가 상점에게 노출되지 않은 상태에서 상점은 고객의 신원확인 및 구매 내용을 확인
- 지불중계기관은 판매자가 전송한 결제정보가 실제 구매자가 의뢰한 결제 정보인지 확인



안전결제 vs. 안심클릭


이니페이 플러그인 도움말
*각 메뉴 또는 내용 클릭하시면 해당 도움말을 확인할 수 있습니다.
Secure Internet Life
INICIS
카드선택 → 카드정보입력/인증 → 정보확인 → 결제완료
신용카드 – 카드선택
신용카드
계좌이체
무통장입금
휴대폰결제
전화결제
OK 캐쉬백
상품권
상품명 월드컵 축구공
상품금액 25,000원
고객님께서 사용하실 카드의 결제서비스를 선택하여 주십시오.
01
안전결제(ISP) 국민, BC, 우리
안심클릭 엘지, 삼성, 신한, 현대, 외환, 롯데, 하나, 씨티, 한미, 신세계, 광주, 전북, 수협, 산업, 조흥, 제주
일반카드결제 농협, 해외비자, 해외마스터, 해외JCB, 해외아멕스, 해외다이너스
결제금액이 30만원 이상일 경우 공인인증서가 필요합니다.
공인인증제도
'05년11월부터 의무시행
ENGLISH →
02 다 음
취 소
INICIS
이니페이는 항상 신뢰와 기술로 고객님과 함께 합니다.
copyright ©2004-2007 INICIS All rights reserved.
신용카드 결제서비스는
신용카드를 이용해 인터넷 쇼핑몰 또는 컨텐츠몰에서 물품(컨텐츠)를 구매하는 것으로 신용카드사에 따라 다양한 인증형태가 있습니다.
01 이용하시고자 하는 카드에 해당하는 카드 결제서비스를 선택하세요.
A 안전결제(ISP)
국민, BC, 우리카드의 경우 ISP 인증서를 다운받아야 사용할 수 있습니다.
결제과정에서 ISP 인증서를 다운로드받을 수 있습니다.
30만원 이상의 거래금액에 대해서는 공인인증을 받으셔야 합니다.
공인인증제도 도움말을 참조하시기 바랍니다.
신용카드의 경우 1,000원 이상의 거래만 가능하며 5만원 미만의 경우 할부개월을 선택할 수 없습니다.
02 카드의 결제 서비스를 선택하신 후 다음 버튼을 클릭해주세요.
× 닫 기
› 계 속

안전결제 vs. 안심클릭

- **SET**
  - 처리절차가 복잡하여 활용되지 않음
- **안전결제**
  - 마스터카드에서 개발
  - ISP 안전결제 정보를 PC에 저장, 전자서명 수행
- **안심클릭**
  - 비자카드에서 개발
  - 인증정보를 사용자 PC 대신 신용카드사에 저장
  - 사용자 결제시 쇼핑몰의 결제창 대신 신용카드사의 안심클릭 결제창을 띄움
  - 패스워드 또는 공인인증서로 인증

3. 전자투표

- **전자투표란?**
  - 종이 투표용지를 사용하지 않고 컴퓨터, 통신망 등 전자장비를 이용하는 투표방식
- **장점**
  - 편리성, 효율성
  - 선거경비 감소
  - 감소하고 있는 투표율을 높이기 위한 대책

전자투표 방식

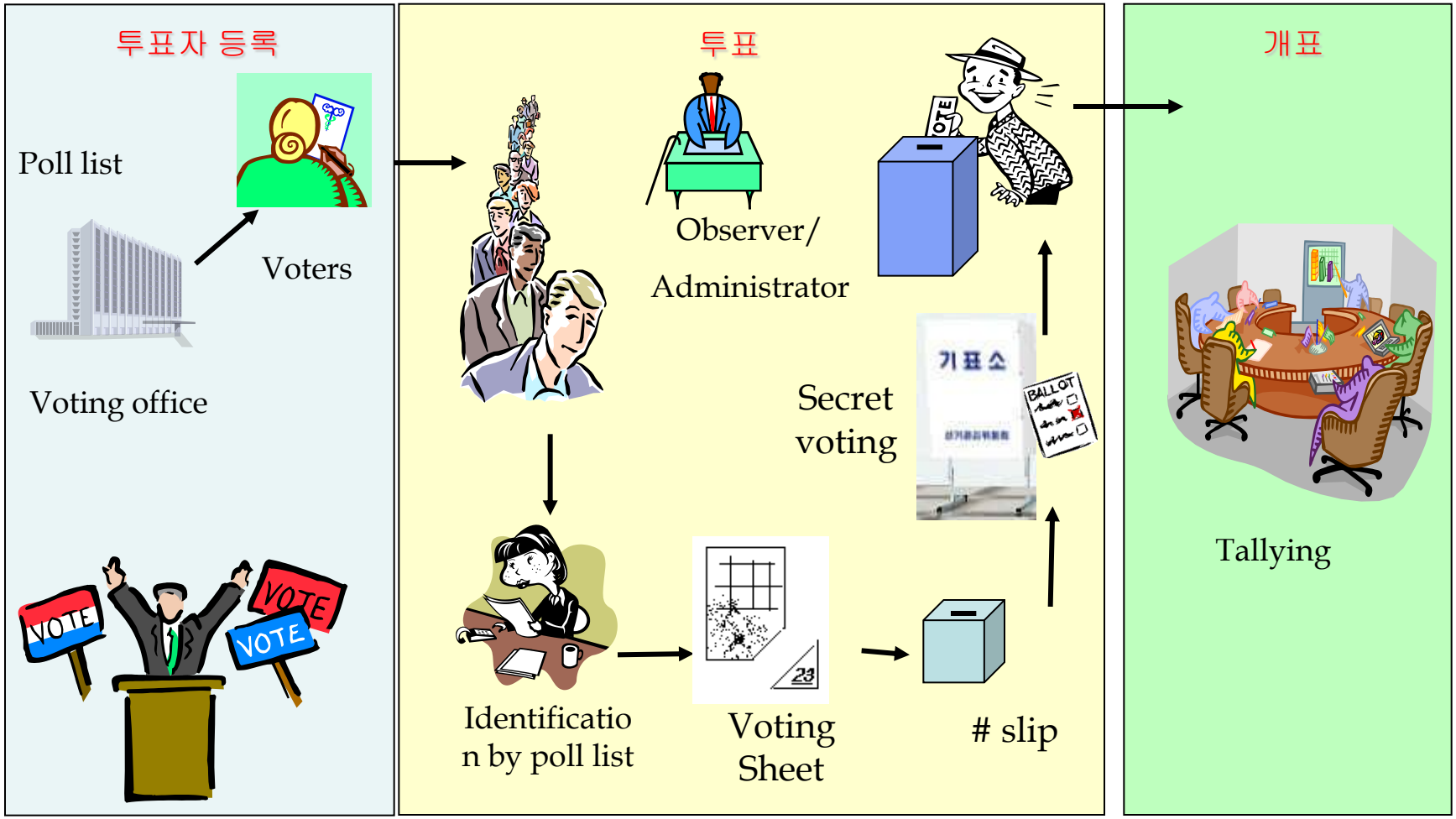
- 투표소 투표 방식
  - 터치스크린 방식의 키오스크에서 투표
  - 컴퓨터 이용하여 투표
- 원격투표 방식
  - 인터넷 이용하여 투표
  - 휴대전화 SMS 이용

터치스크린 투표시스템

전자투표 적용 사례

- 외국의 사례
  - 인도, 노르웨이, 미국, 벨기에, 스위스, 영국, 에스토니아, 호주 등 20여개국에서 실시중
- 국내 사례
  - 선거관리위원회에서 전자투표 대행
  - 당내 경선 등에서는 인터넷 투표, 모바일 투표, 터치스크린 투표 등 다양한 방식을 적용
  - 대선, 총선 등 국가규모의 선거에서는 아직 적용되지 못함. 정치권의 합의가 필요

투표 시나리오


투표자 등록
Poll list
Voters
Voting office
VOTE
VOTE
VOTE
투표
Observer/
Administrator
Secret
voting
기표소
BALLOT
Identificatio
n by poll list
Voting
Sheet
slip
개표
Tallying

전자투표 보안요구사항

- 비밀성
- 이중투표 방지
- 정확성과 검증성
- 공정성
- 강인성
- 매표 방지, 강압투표 방지

- 효율성, 편리성

인터넷 투표의 접근방법

- **은닉서명(blind signature)**을 이용하는 기법
  - 은닉서명으로 투표관리자가 추적할 수 없는 투표용지를 발급
- **믹스넷(mixnet)**을 이용하는 기법
  - 암호화된 투표용지를 암호학적으로 섞은 후 개표하는 방법
- **준동형암호(homomorphic encryption)**를 이용하는 기법
  - 개별적 투표용지를 복호화하지 않고 전체 투표용지를 합쳐서 한번에 복호화하는 방법